U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-65
Phone: (202) 267-1798
Fax: (202) 267-2598

COMDTINST 5375.1A
06 APR 04

COMMANDANT INSTRUCTION 5375.1A

Subj: LIMITED PERSONAL USE OF GOVERNMENT OFFICE EQUIPMENT

Ref: (a) Standards of Ethical Conduct, COMDTINST M5370.8 (series)
(b) Personal Use of Government Office Equipment, DHS MD Number 4600.1

1. PURPOSE. This Instruction refines policy on personal use of government office equipment by all Coast Guard employees.

2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, assistant commandants for directorates, the Judge Advocate General, and special staff offices at Headquarters shall ensure compliance with the provisions of this Instruction. Internet release authorized.

3. DIRECTIVES AFFECTED. Limited Personal Use of Government Office Equipment, COMDTINST 5375.1, is hereby cancelled.

4. DISCUSSION. Since the inception of the original policy on limited personal use of government equipment, Information Technology (IT) systems and our IT infrastructure have become integral components of daily operational and business activities in the CG. While limited use of the IT infrastructure and the Internet by one person did not significantly impact official business, the aggregate use by many has negatively impacted the network.

5. AUTHORITY. Personal Use of Government Office Equipment, DHS MD Number 4600.1; and, Article 92, Uniform Code of Military Justice (UCMJ).

DISTRIBUTION – SDL No. 141

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1	1	1	1	1	1	1		1	1		1	1	1	1	1	1		1		1					
B	1	8	10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1		1
D	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
E	1	1	1	1				1		1	1	1	1	1	1		1		1	1			1	1		
F																	1	1	1							
G		1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

6. DEFINITIONS.

   a. Government office equipment: Equipment and systems purchased and/or owned by the government. Includes, but is not limited to, IT equipment, pagers, Internet services, email, library resources, telephones, facsimile machines, photocopiers, and office supplies.

   b. Personal use: Activity that is conducted for purposes other than accomplishing official, educational or otherwise authorized activity.

   c. Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. IT includes, but is not limited to, desktop computers, personal computers, laptops, handheld computers, Personal Digital Assistants (PDAs), related peripheral equipment, and software.

   d. Non-work time: The time when CG or DHS users are not performing an activity for the benefit of the CG or the Department and under the control or direction of the service or the Department. Examples of non-work time include off-duty hours such as lunch periods, authorized breaks, before or after a workday, weekends or holidays, but only if your duty station would normally be available to you at such times.

7. POLICY.

   a. Employees must be authorized to use government office equipment for official Government business before it is available for limited personal use.

   b. Personal use of government office equipment, as those terms are defined in paragraph 6 above, is limited to 30 minutes of non-work time over a 24-hour period for all authorized users.

   c. Managers and supervisors may further restrict personal use based on the needs of the command or office, or problems with inappropriate use.

   d. All CG personnel must comply with the requirements of this Instruction when telecommuting, in addition to existing policy regarding telecommuting.

   e. This Instruction shall be referenced in all CG Information User Agreements.

   f. Any incident (suspected/actual) must be reported to the local IT support staff and Information System Security Manager/Officer (ISSM/ISSO), including accidental introduction of virus/worm, malicious software, accidental release of sensitive information, or anything that compromises the confidentiality, integrity, availability, authentication, and non-repudiation of the CG enterprise IT infrastructure.

8. PROHIBITED USES. This Instruction is a lawful general order, punishable under Article 92 of the Uniform Code of Military Justice. Violations of this Instruction may result in administrative and disciplinary action against military personnel. It is authority for taking adverse personal actions against civilian employees. Violations of this Instruction may result in CG personnel being held

financially liable for the cost of prohibited or inappropriate personal use of government office equipment. The following personal use of government office equipment is **prohibited:**

a. Using government office equipment to view, download, store, display, transmit or copy any materials that are sexually explicit, or are predominantly sexually oriented.

b. Loading personal or unauthorized software onto a government computer or other government office equipment.

c. Making unauthorized configuration changes to a government computer system (without going through the proper change configuration process (e.g., ECP, LCCB)).

d. Downloading, importing, copying or transmitting large data files (400 KB).

e. Subscribing to or downloading streaming data services (e.g., streaming video, streaming audio, stock tickers) or other automatic Internet data services.

f. Engaging in any outside fund raising activity, endorsing any product or service, or participating in lobbying or other prohibited partisan political activity.

g. Using government equipment as a staging ground or platform to gain unauthorized access to other systems.

h. Using government office equipment for commercial purposes or to support a private or personal business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal or private business also precludes employees using government office equipment to assist relatives, friends, or other persons in such activities.

i. Acquiring, reproducing, transmitting, distributing, or using any controlled information including computer software and data, protected by copyright, trademark, privacy laws or other proprietary data or material with other intellectual property rights beyond fair use, or export-controlled software or data.

j. Deliberate introduction or failure to report accidental introduction of viruses, worms, or other malicious software.

k. No personal computers will be attached to any Coast Guard Network.

9. INAPPROPRIATE USES. The following personal use of government office equipment, not listed in paragraph 8 above, is **inappropriate** and may result in adverse administrative actions against CG personnel:

a. Making personal long distance telephone calls – There are three exceptions:

(1) In an emergency;

(2) Brief calls within the local commuting area to locations that can only be reached during working hours (e.g., car repair shop, doctor); and

(3) Brief calls home within the local commuting area (e.g., to arrange transportation, check on a sick child).

b. Creating, copying or transmitting any material or communication that is illegal or offensive to fellow employees or to the public, such as hate speech, material that ridicules others based on race, creed, religion, color, sex, disability, national origin, or sexual orientation.

c. Creating, copying, or transmitting chain letters or other mass mailings (10 or more addressees), regardless of the subject matter.

d. The following types of Internet sites shall not be accessed using CG computers and networks (these are by way of example and not by limitation):

(1) Dating services (i.e., match.com).

(2) Personal shopping (i.e., amazon.com, ebay.com) (due to overhead of continuous certification processing).

(3) Streaming data to include stock prices, streaming audio and/or videos content.

(4) Music, gaming, and gambling oriented content.

(5) Personal e-mail sites (Hotmail, AOL, MSN, Yahoo, etc. – these circumvent CG firewall / virus security measures).

(6) Chat rooms (MSN Messenger, AIM, ICQ, etc). (note: CG Central has a chat capability for business needs that remains internal to the CG network).

e. Threats to CG networks and possible compromise of CG Data requires that the following types of applications not be used (including the use during Remote Access Sessions (RAS):

(1) File sharing.

(2) Internet chat programs (e.g., AOL, Yahoo or MSN Instant Messenger type programs, including any JAVA based versions).

(3) Peer-to-Peer programs (e.g., Kazaa, Gnutella, Napster).

(4) Unauthorized outbound Remote Desktop Procedures connections (RDP).

Note: As new threats arise that impact the information assurance posture of the CG, they will be published and the Information Assurance program will implement appropriate protection strategies.

10. LOCAL RESTRICTIONS. Commanding Officers and Officers in Charge may be required to reduce personal usage due to bandwidth restrictions as a result of increased operational tempo or degradation of network services. For example vessel bandwidth at sea is severely limited, which may lead to a more restrictive personal usage policy (e.g., no attachments to email authorized).

11. ENVIROMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and have been determined to be not applicable.

12. FORMS/REPORTS. None.

T.W. ALLEN /s/
Vice Admiral, U.S. Coast Guard
Chief of Staff